TAKING A FRESH LOOK AT PUBLIC SAFETY'S SPECTRUM NEEDS: TOWARD A NEXT GENERATION STRATEGY FOR PUBLIC SAFETY COMMUNICATIONS

Dale Hatfield
University of Colorado
Interdisciplinary Telecommunications Program

Phil Weiser
University of Colorado School of Law and
Interdisciplinary Telecommunications Program

EXECUTIVE SUMMARY

As we approach the completion date for the digital transition, policymakers have an opportunity to take a careful and fresh look at the challenge of developing a next generation public safety communications network. Since the mid-1990s, the promise of providing additional spectrum in the 700 MHz band to public safety agencies has remained unfulfilled and many of the plans for public safety communications have either stalled or remained focused on 1990s technology. By examining innovations in wireless communications over the last decade, this White Paper suggests that the best policy for public safety agencies is to look beyond simply using more spectrum dedicated to their private land mobile radio (LMR) systems.

As explained in this White Paper, the optimal public safety communications architecture is a flexible system that accommodates different technologies. In particular, an ideal system would incorporate traditional LMR systems into a broader architecture that includes satellite, terrestrial, and emerging wireless broadband networks. Particularly with the advent of mobile satellite services' ancillary terrestrial component offering (which can switch seamlessly between satellite and terrestrial networks), the benefits of this hybrid approach are substantial. To advance this vision, policymakers should ensure that satellite and terrestrial providers are afforded the opportunity—through pro-market and innovative spectrum policies—to develop effective offerings for public safety agencies.

I. Introduction

We have prepared this White Paper, on behalf of Mobile Satellite Ventures LP (MSV),[1] to explain how the recently authorized "**ancillary terrestrial component**" (ATC) of mobile satellite services provides an important and significant option for public safety agencies. Notably, MSV is already providing service to a number of public safety agencies today. Beginning within the next couple of years, after completing the deployment of an ATC service, MSV will be able to expand this service and offer it more efficiently to public safety agencies across the United States. By appreciating the bigger picture of how public safety agencies can use such offerings in addition to traditional land mobile radio (LMR) networks, policymakers can promote the development of a realistic and effective nationwide interoperable broadband mobile communications system for public safety agencies.

This White Paper proceeds in three parts. First, we outline the requirements for an ideal public safety network, noting the often cited shortcomings of traditional commercial providers. Second, we explain how public safety agencies can utilize networks provided by commercial providers—particularly hybrid satellite and terrestrial systems—to satisfy the relevant requirements in a cost-effective fashion. Finally, we explain how policymakers can facilitate the transition to such optimal hybrid networks.

[1] MSV is the entity authorized by the Federal Communications Commission in 1989 to construct, launch, and operate a Mobile Satellite Service system in the L-band. MSV's licensed satellite (AMSC-1) was launched in 1995, and MSV began offering service in 1996. MSV is also the successor to TMI Communications and Company, Limited Partnership (TMI) with respect to TMI's provision of L-band MSS in the United States. Today, MSV offers a full range of land, maritime, and aeronautical satellite services, including voice and data, using both its own U.S.-licensed satellite and the Canadian-licensed L-band satellite licensed to Mobile Satellite Ventures (Canada) Inc. In November 2004, the Federal Communications Commission authorized MSV to supplement its satellite service with ATC. See Mobile Satellite Ventures Subsidiary LLC, Order and Authorization, DA 04-3553 (Chief, International Bureau, November 8, 2004).

II. Requirements For A Next Generation Public Safety Network

In the wake of 9/11 and an emerging awareness of the shortcomings of current public safety communications networks, most policymakers are very familiar with the arguments for developing a next generation (i.e., broadband and interoperable) mobile radio network. Thus, rather than focus on the particular applications and rationale for such a network, this Part explains the key requirements of any such network. In particular, we explain the need for (A) ubiquitous access; (B) reliability; (C) interoperability; (D) configurability; and (E) security. In so doing, we make a special effort to acknowledge the criticisms traditionally leveled at commercial wireless providers.

A. Ubiquitous Access

The fundamental requirement for public safety mobile radio networks is that they must function in all areas served by first responders. The need for ubiquitous access is a notorious shortcoming of modern commercial mobile radio networks, which often do not serve more remote areas.[2] As commercial providers underscore, the territory they do serve often includes 90% of the population. Because of the increasingly urbanized nature of the nation, however, this coverage can be achieved while covering less than 10% percent of the U.S. land area. Given this limited geographic reach and the lack of coverage for the other 10% of the population, public safety agencies traditionally have eschewed reliance on commercial systems and have developed their own private land

[2] Mary Greczyn, *FCC Weighs Whether To Scrap 20-Year-Old Cellular Mandates*, COMMUNICATIONS DAILY (August 7, 2002) (reporting that digital cellular networks reached only around 50% of the population).

mobile radio (LMR) systems. Significantly, even many private LMR systems operated by public safety agencies do not cover their entire territory. The New Mexico State Police's system, for example, cannot reach 15% of the state—and is limited to voice communications.[3]

The second aspect of ubiquitous coverage involves ensuring service in buildings. Historically, the lack of radio communications ability within buildings represented a notable failing of public safety LMRs—and one that has led to tragic results during emergency situations such as 9/11.[4] To respond to this failing, some cities have required in-building coverage plans as part of any new construction (such as the installation of bi-directional amplifiers). In-building systems can be expensive, however, with major high rise buildings requiring an investment of $1-$2 million.[5]

B. Reliability

For public safety agencies, the second critical requirement is that "mission critical" networks be able to survive and continue to operate during natural or man-made disasters, such as earthquakes, fires, or a high-powered blast caused by a bomb. In many cases, traditional commercial networks are not engineered to withstand such disasters—either because they are not protected or because they do not have sufficient generation capacity or battery back-up to stay online if the power grid goes down. Moreover, even if available, commercial systems are often overloaded by calls during emergencies; as one

---

[3] James Careless, *Speak Easy: Technologies To Improve Two-Way Communications for First Responders*, FRONTLINE FIRST RESPONDER (June 2003) (http://www.msvlp.com/pr/pdf/speakeasyarticle.pdf).
[4] *Increasing FDNY's Preparedness*, August 19, 2002 (www.nyc.gov/html/fdny/html/mck_report/toc.html).
[5] Public Safety Wireless Network Program, *Public Safety In-Building/In-Tunnel Ordinances and Their Benefits to Interoperability Report* (November 2002) (http://www.safecomprogram.gov/NR/rdonlyres/2311FAAD-18DE-4EA9-BC5A-6C99CC24BAFA/0/In_Building_In_Tunnel_Ordinances_Report.pdf).

report explained, "[e]xperience has shown that such systems are often the most unreliable during critical incidents when public demand overwhelms the system."[6] In short, whether through private or commercial wireless systems, it is clear that public safety agencies need access to a system that will be available during emergencies and that will afford them with priority access.

C. Interoperability

As numerous policy observers and policymakers have emphasized, the lack of interoperability among public safety agencies remains a grave concern.[7] As the Federal Communications Commission has defined the issue, interoperability is "[a]n essential communications link within public safety and public service wireless communications systems which permits units from two or more different entities to interact with one another and to exchange information according to a prescribed method in order to achieve predictable results."[8] Stated more simply, interoperability means that two (or more) emergency service providers—say, a paramedic and a fire fighter—can communicate with one another in an efficient, reliable, and secure fashion. Given the American system of government, with thousands of local agencies that enjoy local autonomy, it should not be surprising that different jurisdictions (as well as,

---

[6] National Task Force on Interoperability, *When They Can't Talk, Lives Are Lost* (February 2003) (http://www.agileprogram.org/ntfi/ntfi_brochure.pdf).

[7] *See, e.g.*, Government Accountability Office, Protecting Structures and Improving Communications During Wildland Fires 24 (April 2005) (http://www.gao.gov/new.items/d05380.pdf) ("The lack of communications interoperability among firefighting and other first-responder agencies can impair their ability to respond to emergencies quickly and safely, and cost lives among responders and those they are trying to assist.").

[8] *The Development of Operational, Technical, and Spectrum Requirements For Meeting Federal, State, and Local Public Safety Agency Communication Requirements Through the Year 2010*, First Report and Order, 14 FCC Rcd 152 ¶ 76 (1998).

unfortunately, agencies within the same jurisdiction) have often made decisions that inadvertently do not promote this goal.

In looking back at the numerous inquiries into the causes of the continuing lack of interoperability, several themes emerge as predominant. First, many jurisdictions lack the funds to upgrade their systems (that are often 20-40 years old) and, more fundamentally, are unable to plan effectively for their wireless communications needs. Second, local public safety administrators (either managers like the Chief of Police or the relevant IT professional working in an agency) are often attached to their current approaches and unwilling to give up control to facilitate a greater sharing of resources and technology. In this respect, achieving interoperability is not simply a matter of upgrading equipment, but also of changing the culture of operating in isolation and without full regard for how other public safety agencies operate. To be sure, there are some notable successful ventures that have galvanized regional cooperation between different agencies, such as the Capital Wireless Integrated Network (CapWIN) project that has brought together over 40 local, state, and federal public safety agencies in the Washington, D.C. metro area into a system that provides important real-time communication abilities and access to government databases. Such projects, however, require a system of effective governance involving a number of discrete agencies willing to coordinate their radio equipment needs. Notably, as many other failed initiatives demonstrate, ambitious visions of developing a single system to be used by all relevant

agencies are very difficult to achieve and thus more flexible approaches are far more likely to be successful.[9]

A third major cause of limited interoperability is that many agencies cannot communicate with one another because they use equipment with incompatible (and proprietary) technology. In some cases, these sorts of challenges can be addressed by developing intermediary patches—i.e., a dispatch center (using "bridge equipment") that can interconnect different systems—but such "second best" solutions are expensive and inefficient compared to more rationally designed systems.

Although none have taken hold completely, there are a number of efforts that have attempted to overcome the lack of common standards and to develop ones to facilitate interoperable public safety communications. Notably, the APCO-sponsored Project 25 standard and the European-developed TETRA standard have both sought to advance this goal; more recently, the international "Project MESA" initiative has begun to develop a next generation standard. As for the exchange of data, a coalition of first responders is now working to develop an Extensible Markup Language (XML)-based standard (i.e., the Emergency Data Exchange Language (EDXL)) to enable the panoply of different agencies that might be called to the scene of an accident (i.e., public safety, transportation, and medical personnel) to share information with one another.[10] In its effort to facilitate interoperability, the Federal Communications Commission chartered an advisory committee (the Public Safety National Coordination Committee) that has recommended technical and operational standards for spectrum that will be made

[9] National Task Force on Interoperability, *Why Can't We Talk: Working Together to Bridge The Communications Gap to Save Lives, Supplemental Resources* 19-22 (February 2003) (http://www.agileprogram.org/ntfi/ntfi_supplemental.pdf) (detailing Colorado's failed approach).
[10] Diane Frank, *First Responders Seek Common Lingo*, FEDERAL COMPUTER WEEK (March 15, 2004) (http://www.fcw.com/article84556).

available to public safety agencies.[11] Finally, the Department of Homeland Security's SAFECOM initiative has developed a "statement of requirements" that, in the words of SAFECOM's Director, provide an "architectural framework for future interoperable public safety communications."[12]

The final cause of limited interoperability is that local public safety agencies often lack access to radio spectrum in the same frequency bands used by sister agencies. As a result, public safety agencies—which use any one of ten different bands of spectrum—often cannot communicate with one another even when using compatible technology. To rectify this situation, many in the public safety community have suggested that the transition to digital television, which will open up 24 MHz of spectrum in the valuable 700 MHz band for public safety uses,[13] should alleviate such concerns. But, to understate matters, it remains "somewhat elusive" whether the transition will be completed by 2006—or even 2009, for that matter—and "no public safety agency can logically budget for equipment that uses radio spectrum that is not yet available for them."[14]

In evaluating the spectrum issue, it is important to make clear that this aspect of interoperability might be unsolvable because different agencies often have good reasons for choosing different bands. In short, there are big differences in propagation characteristics between the lowest frequency band and the higher frequency bands used

---

[11] *See The Development of Operational, Technical, and Spectrum Requirements For Meeting Federal, State, and Local Public Safety Agency Communication Requirements Through the Year 2010,* Fifth Memorandum Opinion and Order, __ FCC Rcd __ (2005) (considering recommendations).
[12] Press Release, Homeland Security First to Define Interoperability Requirements for Nation's First Responder Community (April 26, 2004) (http://www.dhs.gov/dhspublic/display?content=3513).
[13] *The Development of Operational, Technical, and Spectrum Requirements For Meeting Federal, State, and Local Public Safety Agency Communication Requirements Through the Year 2010,* First Report and Order, 14 FCC Rcd 152 (1998); *Reallocation of Television Channels 60-69, the 746-806 MHz Band,* Report and Order, 12 FCC Rcd 22,953 (1997); Balanced Budget Act of 1997, Pub. L. No. 105-33, § 3004, 111 Stat. 251 (1997) (codified at 47 U.S.C. § 337(a)(1)).
[14] *Why Can't We Talk*, supra, at 53.

by public safety agencies; consequently, agencies in, say, mountainous areas have compelling reasons for choosing different bands than those agencies in very different (and possibly adjacent) areas. Thus, even if the FCC could identify adequate available capacity, it would still be unwise to force all public safety agencies into a single band.

D. Configurability and Flexibility

The ability of public safety networks to provide one-to-many communications (think "calling all cars") is essential to their effectiveness. Moreover, it is important that such networks be flexible and configurable so that they can include other groups (say, utilities when damage to an electric grid is involved) on an as-needed basis. In some cases, both of these features—i.e., a one-to-many functionality and an ability to create ad hoc networks of users—were lacking in traditional commercial networks. Increasingly, however, modern commercial networks (which are often software-based and designed for multiple applications) can support applications specialized for first responders, including sophisticated push-to-talk features.

E. Security

For public safety agencies, protecting the privacy of communications and guarding against malicious attacks on their communications services are critical priorities. To keep information private and guard against attacks, secure communications systems must encrypt communications (so that unauthorized users are not able to intercept them) and bilaterally authenticate both remote users and servers (to limit who has access to the system). In an ideal system, encryption keys can be dynamically assigned from a central

management system so that additional users can be added as needed. Again, traditional commercial networks tend to lack sophisticated encryption and authentication capabilities. Going forward, commercial systems, such as the system MSV is developing for its ATC network, will increasingly deploy more sophisticated security features—such as Public Key Infrastructure (PKI)—and allow for applications that can provide additional security (e.g., through the use of stronger encryption, such as NSA Type-1).

III. MSV's Existing Satellite and Future ATC Services Provide Important Benefits to Public Safety Agencies

In evaluating the communication needs of public safety agencies, policymakers should reject the calls for a "one-size fits all" solution and recognize, as the Federal Wireless Policy Committee has put it, that "more than one service may be required to support" a next generation public safety network.[15] In particular, policymakers should promote a hybrid approach that would incorporate LMR systems along with terrestrial, satellite, and emerging wireless broadband systems. Such solutions are only beginning to be tested, but it is increasingly apparent that traditional LMR systems can be provided along with ancillary terrestrial component satellite handsets that automatically switch between cellular and satellite systems (depending on which is available). Moreover, by designing such systems in a modular fashion, they can rely on wireless broadband networks, such as those using WiFi technology as well as still emerging technologies (like the next generation WiMAX standard).

---

[15] Federal Wireless Policy Committee, *Federal Functional Requirements for Commercial Wireless Services* (Dec. 11, 2001) (http://www.fwuf.gov/docs/rev_dec01.pdf); *see also* James Careless, *Speak Easy: Technologies To Improve Two-Way Communications for First Responders*, FRONTLINE FIRST RESPONDER (June 2003) (http://www.msvlp.com/pr/pdf/speakeasyarticle.pdf) (highlighting virtues of a multi-mode solution); Michael McShea & Richard Davis, *A Hybrid Approach*, MISSION CRITICAL COMMUNICATIONS 57 (April 2005); Alan Shark, *Don't Rule Out Either Option*, MISSION CRITICAL COMMUNICATIONS 60 (April 2005) ("no one system can or should meet all jurisdictional mission-critical needs").

The case for relying on commercial systems in general and hybrid satellite-terrestrial systems in particular is that they enable public safety agencies to benefit from the considerable economies of scale and enhanced functionalities that commercial providers can offer. Even under the very best of circumstances, public safety agencies are generally not able to build up the economies of scale and develop the network efficiencies of their commercial brethren. At a minimum, then, public safety agencies should take advantage of opportunities to use commercial systems for at least some of their communications needs. As we explain below, MSV's satellite services in general and its hybrid satellite-terrestrial offering in particular meet the requirements outlined above and are well suited to be a valuable component of public safety wireless systems.[16]

To supplement traditional commercial terrestrial networks, it is critical to incorporate satellite services into public safety wireless systems. First, as the case of the New Mexico State Police demonstrates, satellite technology can assure complete coverage to public safety agencies. In particular, the New Mexico State Police Department has compensated for the lack of ubiquitous coverage and ability to carry data on its private LMR by contracting with MSV for access to a satellite-based solution that provides ubiquitous coverage, reliable push-to-talk services, and access to data communications capabilities. Moreover, with the approved ATC architecture that MSV will begin rolling out for its hybrid satellite-terrestrial system, the price of the service will be substantially less than current satellite systems (on account of its use of mainstream devices as well as more efficient terrestrial systems where appropriate) and will decline dramatically as subscribers adopt it and the network enjoys greater scale economies.

[16] MSV is the leading developer of ATC systems, with 800 different covered claims in its 6 patents received to date and 70 additional patents pending. *See* Press Release, Sixth Comprehensive Patent Issued to Mobile Satellite Ventures (May 18, 2005) (http://www.msvlp.com/pr/news_releases_view.cfm?id=62).

Significantly, even as to one of the advertised strengths of private LMR systems *vis-à-vis* commercial networks—the ability to provide coverage wherever it is needed—hybrid satellite-terrestrial systems can provide the best of both the commercial model as well as the traditional LMR systems. Thus, for carriers looking at the expense of adopting new LMR systems for remote areas and the ongoing costs of maintaining the necessary equipment, a hybrid satellite-terrestrial system provides an exciting alternative.

MSV's network provides a reliable and flexible wireless communications product that will become even more attractive once its ATC service is deployed. Unlike most commercial networks, hybrid satellite-terrestrial systems can be used when the local power grid fails. In particular, hybrid satellite-terrestrial handsets can switch seamlessly between cellular networks (when a base station is operating nearby) and a satellite network (when there are no base stations in the area). In terms of providing priority access, MSV is designing its system so that, in the case of emergency events, the public safety operators can enjoy priority access to the extent necessary to preserve public safety communications. To do so, MSV is incorporating priority-precedence features contained within today's 3 G (and some 2 G) cellular standards.[17] Moreover, with its satellite network, MSV can provide superior call completion rates—even for calls that require cost-to-coast connectivity—when delivering "on network" calls that eliminate (or, in some cases, limit) any dependency on the external wireline network.

[17] The essence of priority and precedence features contained in, or under development for, 3G cellular standards, is that they enable pre-defined user classes to obtain priority access to wireless communications resources. Consider, for example, the enhanced Multi-Level Precedence and Preemption (eMLPP) feature within the Global System for Mobile Communications (GSM) air-interface, which provides for up to five distinct priority classes that (during periods of congestion) allow an "emergency call" to queue for the next available radio channel.

In terms of flexibility and configurability, MSV's hybrid satellite-terrestrial system will allow for the creation of ad hoc user groups that can use push-to-talk functionality and communicate among an interdisciplinary team through a large group dispatch service. Significantly, MSV expects the set-up time for such push-to-talk functionality to be similar to its existing offering, with a range of 1.5-2.0 seconds for talk group initiation and a delay between speakers of about 0.5-0.75 seconds. To be sure, this system may not be appropriate for "shoot-don't-shoot" situations, but it will be entirely adequate for an array of scenarios where push-to-talk systems are used by public safety agencies.

Increasing their reliance on commercial systems such as MSV's hybrid satellite-terrestrial system does not mean that public safety agencies should abandon their existing private LMR systems. Rather, private LMR systems often serve a very useful purpose and should be an important part of a hybrid network architecture. Along these very lines, both mission critical networks and critical infrastructure companies (such as utilities like the Tennessee Valley Authority) have begun to gravitate away from relying solely on their private networks. In particular, a number of entities that previously relied solely on their LMRs have concluded that they should continue to maintain such networks, but rather than upgrade them, they can increase productivity and cut costs by moving towards an integrated architecture that includes commercial wireless networks.

In terms of developing an optimal network architecture, public safety agencies should also be open to taking advantage of advances in wireless broadband technology developed for unlicensed spectrum. A public safety network might employ, for example, current wireless local area network (WLAN) technology (i.e., the 802.11 (WiFi) standard) and, eventually, next generation systems (e.g., 802.16 (WiMAX) systems). To

foster the adoption of such systems by local governments, the FCC recently made available access to spectrum in the 4.9 GHz band. As the FCC stated in its press release, "public safety licensees [can now] use a single, low-cost device to access the 4.9 GHz band, the U-NII band, and the ITS band, allowing them to enjoy savings that are typically limited to the high-volume commercial market."[18] Recognizing this opportunity, some police departments, like that of Salida, Colorado, have adopted solutions based on this technology, saving money and making police officers more productive in the process.[19]

An alternative for providing wireless broadband service is to use ad hoc mesh networking systems. At present, such systems are still in their early stages, but they promise (as one vendor put it) "infrastructure-free, automatically established and maintained, and agile" network architectures.[20] The promised effectiveness of such systems, which rely on a different architecture from today's established wireless technologies, reflects their ability to "forward data one hop at a time over a distributed network of autonomous nodes using new and more reliable and efficient schemes."[21] To limit the need for a widespread deployment of devices with the embedded ability to re-transmit communications (i.e., routers), some cities have deployed systems with transmitters placed on existing infrastructure (like streetlamps) and with intelligent access points to connect to wired infrastructure at particular points. In Garland, Texas, for example, the local law enforcement agency decided to rely on such a network,

---

[18] News Release, FCC Improves Public Safety Access To The Latest Broadband Technology (November 9, 2004) (http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-254117A1.doc).

[19] Jim Renton, *Notebooks and Wi-fi Keep Colorado Cops on the Beat*, MOBILE COMPUTING NEWS (March 8, 2004) (http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40_gci953936,00.html?track=NL-315&ad=477866&Offer=t3.8).

[20] Michael Rauf & Eric Lefebvre, *Keeping the Wireless Connection Running*, 9-1-1 MAGAZINE 58 (Jan/Feb 2003) (http://www.novaroam.com/downloads/nr_911article.pdf)

[21] Rick Merritt, *Darpa Looks Past Ethernet, IP Nets*, EE TIMES (April 26, 2004) (http://www.eet.com/showArticle.jhtml?articleID=19200111).

concluding (after an experimental use of the technology on a limited basis) that installing access points and wireless routers on existing infrastructure would be cheaper than building new transmission towers for either cellular or private LMR transmissions towers.[22] Finally, mesh networking systems, which rely on the basic Internet suite of protocols, can be secured by installing firewalls and other security protections.

In short, an optimal public safety architecture would use a flexible system to accommodate different technologies. As depicted in Figure 1, a public safety agency can use a multi-mode device to access a hierarchy of wireless networks, beginning with a public safety LMR system at the center, then a commercial terrestrial network such as MSV's ATC service and finally a satellite overlay.[23] As noted above, public safety agencies might also choose to integrate a terrestrial wireless broadband network. In any event, the core design principle is that networks should be extensible to other terrestrial networks in addition to the core commercial terrestrial and satellite components.

Both commercial and public safety-driven considerations explain why multi-mode networks are increasingly practical and appropriate. Consider, for example, that today's ordinary consumer wireless devices have two to four bands and tomorrow's devices may well also be able to rely on WiFi networks where available. With an extensible network, the keys to integrating them together are (1) facilitating the back-end integration of the commercial network and one or more LMR systems; and (2) gradually adding new user devices that incorporate satellite connectivity, including push-to-talk. In principle, this

[22] Kris Middaugh, *No More Towers*, GOVERNMENT TECHNOLOGY (May 2004) (http://www.govtech.net/magazine/story.php?id=90189).

[23] Hybrid satellite-terrestrial systems rely on a satellite system that uses the same band of spectrum for an integrated terrestrial system. With such a system, MSV will achieve important spectrum efficiencies and economies of scale which will result in lower cost and more user-friendly consumer equipment than current MSS equipment. Such advancements are critical to deployment of MSV's next generation system and will redound to the benefit of public safety agencies that adopt it.

integration can be accomplished, as shown conceptually in Figure 1, by incorporating a second chipset that would enable the device to use a satellite-adapted version of a mass-market air interface (MMI) such as GPRS, CDMA, OFDM or WiMAX.[24] Based on current estimates, MSV believes that an OEM module incorporating such an additional chipset would cost the public safety user between $40 and $80 per unit. While this is more than the additional cost of the consumer ATC product, it is substantially less than it would be without the economies of scale resulting from the consumer deployment of ATC.

Ultimately, the network depicted in Figure 1 would include an overlay for public safety purposes. Significantly, the concept of such a virtual network could be implemented using the same capabilities that mobile virtual network operators (VNO)[25] use today. In order to ensure control, security, and availability, the core network would dedicate resources to the Public Safety VNO, which would operate the public safety serving-network based on applications and policies of its own choosing. The public safety agency would also have the option not only to integrate a multi-mode radio using physically separate modules, but also to use software-defined radios to switch between different networks and their associated functionalities.[26] In either case, devices like that depicted in Figure 2 would bring together different networks and thus provide (as Figure

[24] Meanwhile, the core radio would continue to have LMR, and could add other capabilities such as the IWIN 162 MHz.

[25] Mobile Virtual Network Operators (MVNOs) lack network infrastructure or licensed spectrum, but instead use another operator's facilities and capacity to provide an alternative service. In a number of cases, they also possess the back-end systems and enhanced functionalities necessary to provide their service.

[26] A reliance on software-defined radio devices would also facilitate greater interoperability by enabling public safety agencies to switch to different frequencies when necessary. As a recent GAO report explained "[s]oftware-defined radios will allow interoperability among different agencies using different frequency bands, different operational modes (digital or analog), proprietary systems from different manufacturers, or different modulations (such as AM or FM)." Government Accountability Office, Protecting Structures and Improving Communications During Wildland Fires 61-62 (April 2005) (http://www.gao.gov/new.items/d05380.pdf).

1 reflects) a far more impressive footprint and greater redundancy than any individual system could offer on its own.

Figure 1

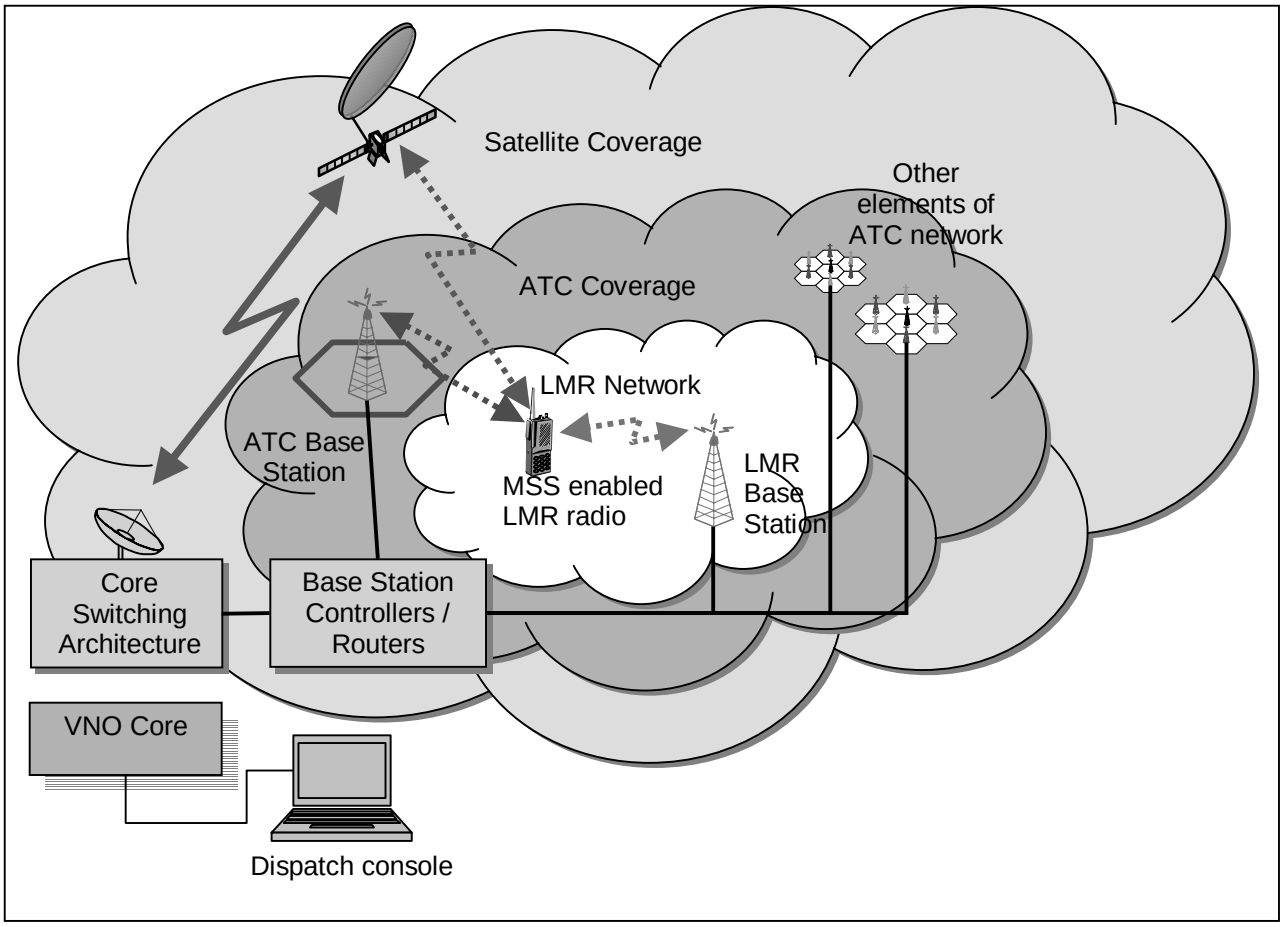
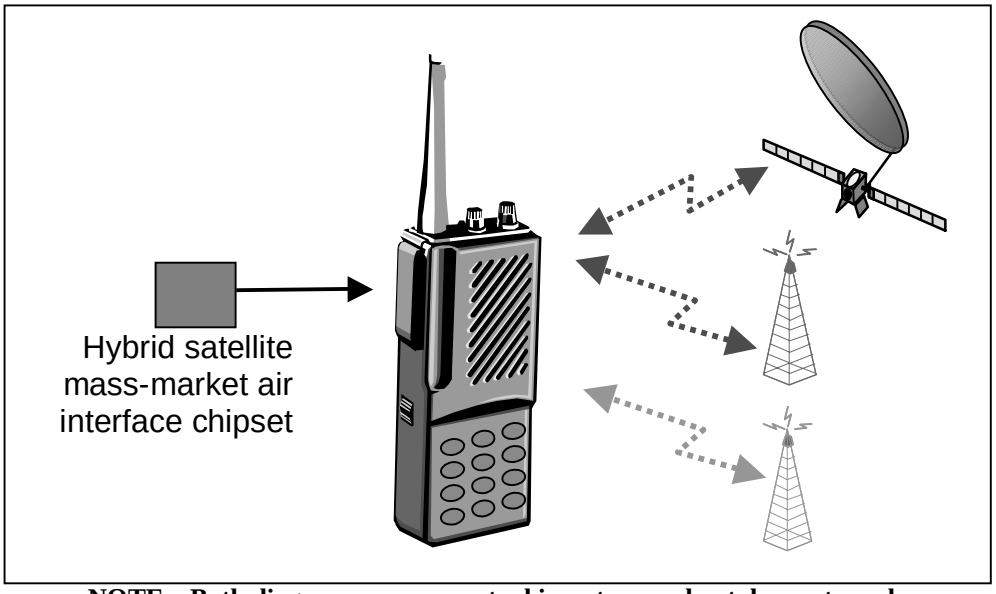


Figure 2



NOTE—Both diagrams are conceptual in nature and not drawn to scale

IV. A Policy Strategy For A Next Generation Public Safety Network

The federal government can play a very important role in facilitating the development of an interoperable broadband mobile communications network for emergency response providers. The best strategy, as suggested above, is not necessarily to promote next generation private LMR systems operated by local public safety agencies. Indeed, committing to such a limited vision might well prove problematic. Rather, the government should appreciate that the ideal mix between public and commercial networks is one it cannot divine in advance and it should thus promote a hybrid model of public safety networks such as that outlined above. To implement such an approach, we recommend two critical regulatory strategies: (A) making available additional spectrum that can be used for public safety applications by commercial providers; and (B) recognizing that a policy of spectrum flexibility benefits public safety agencies by enabling commercial providers to meet their needs.

A. Making More Spectrum Available for Public Safety Purposes

For quite some time, the discussion over "making available additional spectrum for public safety agencies" has focused on dedicating spectrum for private LMR systems operated by specific agencies. Moreover, this discussion has often centered on the 1996 recommendation by the Public Safety Wireless Advisory Committee that 25 MHz of spectrum was needed by 2001 for public safety purposes, with an additional 72.5 MHz required by 2010. Notably, this recommendation assumes both that (1) achieving interoperability and providing mobile broadband capability will require more spectrum to be specifically dedicated to public safety providers and that (2) the transition to digital television will be completed in a timely manner so as to free up spectrum for this purpose. Both recommendations, however, are suspect, thereby raising the question of what alternative strategy policymakers might use to enable public safety agencies to migrate toward a next generation network.

Many policymakers continue to take the traditional perspective of focusing on particular spectrum as designated for certain purposes. In the case of public safety, the historical use of spectrum in and around the 700 MHz band makes it understandable that policymakers would focus on whether additional spectrum in this band is necessary to facilitate the transition toward a next generation public safety communications system. But policymakers should be careful not to indulge the two assumptions questioned above—that providing specialized public safety spectrum is necessarily the best policy and that the digital transition will be completed in a manner that will make available such spectrum in a timely fashion. Rather than indulge such assumptions, we urge

policymakers to think more broadly about what it means to make more spectrum available for public safety uses.

A broader perspective on the issue would appreciate that the Commission's recent action related to enabling public safety agencies to use spectrum in the 4.9 GHz band for wireless broadband is a form of making additional public safety spectrum available. Thinking even more broadly, it is clear that flexible policies related to SMR spectrum—including its decision to allow Nextel to accumulate dispatch licenses—promoted the development of public safety spectrum, as many public safety agencies now use Nextel's services and benefit from its economies of scale. Similarly, with respect to MSV, the Commission's policies authorizing the use of ATC—as well as its efforts now underway to finalize the distribution of surrendered MSS spectrum in the S Band—promise to make available spectrum that will be commercialized in a manner that will benefit public safety agencies.[27]

In short, policymakers should appreciate the importance of committing spectrum to commercial providers who can offer service to public safety agencies. In the case of satellite providers like MSV, it is not merely sufficient for the FCC to allocate spectrum for use by satellite providers, but it is also critical for it to provide certain and stable assignments of satellite spectrum. Only with such stable assignments, and the ability for providers to undertake significant investments over a period of time, will satellite providers be able to deploy innovative offerings like a hybrid satellite-terrestrial system that will ultimately benefit public safety agencies as well as other consumers.

[27] The Commission expressly recognized the public safety benefits of ATC in authorizing its use, concluding that "ATC may enhance the nation's overall ability to maintain critical telecommunications infrastructure in times of crisis or disaster." *Flexibility for Delivery of Communications by Mobile Satellite Service Providers in the 2GHz Band, the L-Band, and the 1.6/2.4 GHz* Bands, Report and Order, 18 FCC Rcd 1962, ¶ 29 (February 10, 2003).

B. A Policy of Spectrum Flexibility Benefits Public Safety Agencies

It is crucial that policymakers appreciate how promoting spectrum flexibility will greatly benefit public safety agencies. As the Spectrum Policy Task Force Working Group on Spectrum Rights and Responsibilities explained the vices of the old approach:

> From the Commission's experience with command-and-control regulation, it is apparent that overregulation can deter both efficiency and innovation. The highly regulated nature of certain services has tended to discourage technological change because the means of providing permissible services are narrowly defined in terms of current and outdated technology. Moreover, in cases where licensees are limited in what services they are permitted to offer, they have no incentive to seek out a higher valued use for the spectrum.[28]

The Commission's new perspective on spectrum policy takes a fairly critical perspective toward the classic "wise man" restrictions on how spectrum can be used and instead calls for "a light touch and a sense of humility" in developing rules that restrict uses of the spectrum.[29] Thus, as the FCC's Spectrum Policy Task Force concluded, the Commission should look "to increase opportunities for technologically innovative and economically efficient spectrum use, spectrum policy must evolve toward more flexible and market-oriented regulatory models."[30]

By reforming its traditional policy toward spectrum management, the Commission will, as Chairman Martin explained, move toward a model of "flexible allocations (that are technology and service-neutral)" of spectrum licenses.[31] This model,

---

[28] Federal Communications Commission Spectrum Policy Task Force, *Report of the Spectrum Rights and Responsibilities Working Group* 11 (November 15, 2002) (http://www.fcc.gov/sptf/files/SRRWGFinalReport.pdf).
[29] Jonathan S. Adelstein, *New Frontiers in Wireless Policy: A Framework for Innovation* 3 (April 9, 2003) (http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-233139A1.pdf).
[30] Federal Communications Commission Spectrum Policy Task Force, *Spectrum Policy Task Force Report* 3, ET Docket No. 02-135 (November 15, 2002).
[31] Kevin J. Martin, *U.S. Spectrum Policy: Convergence or Co-Existence?* (March 5, 2002) (http://www.fcc.gov/Speeches/Martin/2002/spkjm202.html).

which the Commission has begun promoting through initiatives such as its Secondary Markets Order,[32] promises to "create strong incentives for making use of excess capacity" of spectrum already allocated in inflexible ways.[33] Significantly, by continuing to make progress on spectrum reform more generally, policymakers can assist public safety agencies in particular by helping to make the network architecture outlined above more effective and less expensive.

[32] *Promoting Efficient Use of Spectrum Through Elimination of Barriers to the Development of Secondary Markets*, Report and Order, 18 FCC Rcd 20,604 (2003).
[33] Kevin J. Martin, *U.S. Spectrum Policy: Convergence or Co-Existence?* (March 5, 2002) (http://www.fcc.gov/Speeches/Martin/2002/spkjm202.html).

CONCLUSION

Policymakers now have an opportunity to take a broad and careful examination of the best approach for enabling public safety agencies to develop a next generation network. This approach, contrary to the traditional thinking on the subject, should not be centered on how much spectrum in the 700 MHz band needs to be dedicated specifically for public safety uses. Rather, policymakers should appreciate that a flexible, integrated architecture that relies on more than simply LMR systems can best serve many public safety agencies. To promote this system, policymakers should focus on making spectrum *generally* available for broadband uses, whether via unlicensed WiFi-like systems, licensed commercial carriers, or satellite providers (including those using hybrid satellite-terrestrial networks with the aid of ATC technology).

In short, by implementing effective spectrum policies and encouraging the developing of hybrid solutions, policymakers can advance the vision of a next generation public safety network far more effectively than waiting until it can assemble the sufficient spectrum in the 700 MHz band to enable public safety agencies to deploy their own LMR systems. By promoting a public safety network where agencies can use spectrum from commercial providers, unlicensed bands as well as from the spectrum dedicated to their private LMRs, public safety agencies will gain the benefits of a modern, innovation-rich, low cost network. In particular, public safety agencies will benefit from modular, extensible networks that can take advantage of cutting edge applications that ride on either their private LMR, a commercially provided, or an unlicensed wireless broadband network.

Dale Hatfield is an Adjunct Professor of Telecommunications at the University of Colorado and an internationally recognized expert, teacher, and consultant on telecommunications technology and policy. Over his distinguished career in both the public and private sector, he founded a very successful consulting firm and served as the Federal Communications Commission's Chief of the Office of Engineering and Technology, Chief Technologist, and Chief of the Office of Plans & Policy. Professor Hatfield's many honors include: a Department of Commerce Silver Medal for contributions to domestic communications satellite policy, the Attorney General's Distinguished Service Award and the FCC's Gold Medal Award for distinguished service.

Phil Weiser is an Associate Professor of Law and Telecommunications at the University of Colorado and the Founder and Executive Director of the Silicon Flatirons Telecommunications Program. After graduating from New York University School of Law, Professor Weiser served as a law clerk to the Tenth Circuit Court of Appeals Judge David M. Ebel and to United States Supreme Court Justices Byron R. White and Ruth Bader Ginsburg. Before taking his position at CU, Professor Weiser served as the Senior Counsel for Telecommunications Policy to Joel Klein, Assistant Attorney General, Antitrust Division, at the U.S. Department of Justice. Professor Weiser teaches and writes widely on information policy issues and is the author (with Jon Nuechterlein) of "Digital Crossroads: American Telecommunications Policy In the Internet Age (MIT Press 2005)."